Amendments to the Drawings:

The attached drawing sheet includes a new drawing to be added to the application as Figure 7. This new figure is being added in response to the Examiner's requirement that a figure be provided showing, *inter alia*:

- means for connection to the remote computer comprising a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer, and
- the cryptographic module being provided on an external smart card.

No new matter has been added. This is further described in the Remarks section of this paper.

Attachment: One new drawing sheet (new Figure 7)

REMARKS

Claims 1-19, 24-30, and 32-52 are now pending in the application. The specification text and claims 19, and 47 have been amended, and new claims 51-52 and new Figure 7 have been added to the application, without introduction of new matter. Favorable reconsideration is respectfully requested in view of the above amendments and the following remarks.

The courtesy extended to Applicant's representative in a personal interview conducted on November 30, 2007 is noted with appreciation. During the interview, the Examiner and the undersigned attorney discussed the objection to the specification and figures, and the claim rejections under 35 U.S.C. §§ 112, 101, 102, and 103. In particular, Applicant's representative identified those portions of the specification that support the language in claims 1, 7, 19, 28, 36, and 44 to which the Office objects. As no agreement was reached concerning this issue, it was not possible to reach agreement concerning the rejections under 35 U.S.C. §§112, 102, and 103. The Examiner also explained to the undersigned attorney his reasons for re-issuing a rejection of claim 19 under Section 101, and for newly issuing that rejection against claims 47-50. These and other aspects of the conversation are included in the following remarks.

The drawings were objected to under 37 CFR 1.83(a) as allegedly failing to show a number of features presently recited in claims 7, 8, 15, and 44. The various aspects of the Office's objection are traversed in the following:

The Office alleges that "means for communicating over a wireless interface with a wireless communications network" and "means for connection to a remote computer without involving the wireless communications network", both recited in claim 7, are not shown in the figures. This allegation is believed to have been made in error: The "means for communicating over a wireless interface with a wireless communications network" is depicted in each of Figures 1, 4, and 5 as the mobile station (MS) 30. It is well known that mobile stations communicate over a wireless interface with a wireless communications network. As for the "means for connection to a remote computer without involving the wireless communications network", this is depicted in each of Figures 1 and 4 as the line that connects the PC's CSP* 26 with the mobile station's security manager 30. This feature is also depicted in Figure 5 as the line that connects the PC's CT* 76 with the mobile station's security manager 30. Therefore, no drawing changes are believed to be necessary to address this aspect of the Office's objection.

The Office further alleges that "A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network, and comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface", as recited in claim 44, is not shown in the figures. This allegation is believed to have been made in error: "A mobile communications device, the mobile communications device being able to communicate over a first wireless interface with a telecommunications network ..." is shown in each of Figures 1, 4, and 5 as the mobile station (MS) 30. It is well known that mobile stations are devices that are able to communicate over a wireless interface with a telecommunications network. As for the mobile communications device "comprising a cryptographic module to provide cryptographic functionality for use in communications over the first wireless interface", this is depicted in each of Figures 1, 4, and 5 as the SIM-WIM card 32, which, as described on page 5, lines 12-15, houses the cryptographic module in the depicted in embodiments. Therefore, no drawing changes are believed to be necessary to address this aspect of the Office's objection.

The Office further alleges that "means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer" as recited in original claim 8, and "wherein the cryptographic module is provided on an external smart card" as recited in original claim 15, are not shown in the figures. In response to these objections, Applicant herewith submits a new Figure 7. No new matter has been introduced by this amendment, since all of the features depicted in Figure 7 can either be found in originally filed Figure 1, or described in the specification, such as in originally filed claims 8 and 15. The "means for connection to the remote computer comprises a short-range wireless communications transceiver, for sending signals to and receiving signals from the remote computer" are depicted as the short-range wireless transceivers 703 and 703, interconnected by a two-way arrow to schematically illustrate that the short-range wireless transceiver 703 is for "sending signals to and receiving signals from the remote computer". The aspect "wherein the cryptographic module is provided on an external smart card" is depicted as the external smart card 701.

In order to accommodate the new figure, the specification has been amended in several places to include a brief description of Figure 7 under the heading "Brief Description of Drawings", and to also provide a description of elements 701, 702, and 703 in the Detailed Description of Preferred Embodiments (on page 12).

Having addressed each of the concerns expressed in the Office Action, it is believed that the Drawings are fully in compliance with 37 CFR 1.83(a). Accordingly, it is respectfully requested that the objection to the drawings be withdrawn.

The Office objected to the amendment filed on July 25, 2006 under 35 U.S.C. 132(a) because it allegedly introduces new matter into the disclosure. In particular, the Office objects to amendments that were intended for pages 6, 8, 10, 11, and 12 of the specification. This objection is respectfully traversed.

While Applicant strongly disagrees that the proposed amendments filed on July 25, 2006 introduced new subject matter into the disclosure, the issue was long ago rendered moot by the Office's Advisory Action of August 4, 2006, in which Box 3 has been checked to indicate "The proposed amendment(s) filed after a final rejection, but prior to the date of filing a brief, will not be entered because ... (b) They raise the issue of new matter (see NOTE below); (c) They are not deemed to place the application in better form for appeal by materially reducing or simplifying the issues for appeal ...."

That is, the Office is now objecting to language that is not part of the specification. This being the case, there is nothing that Applicant can do to address the Office's concern. It is therefore respectfully requested that this objection to the specification be withdrawn.

The Office further objects to the specification on the grounds that it does not provide antecedent basis for a number of limitations added to the claims in an amendment filed on January 5, 2006. In conjunction with this objection, claims 1-19, 28-30, and 32-46 stand rejected under 35 U.S.C. §112, first paragraph, as allegedly failing to comply with the written description requirement. The Office's entire explanation of this rejection is: "See objection to specification." Because the rejection under the first paragraph of Section 112 appears to be based on the lack of antecedent basis cited above with respect to the objection to the specification, these two issues are respectfully traversed together.

In order to reduce the number of issues to be resolved on Appeal, Applicant filed an After-Final Amendment on July 25, 2006, in which it was proposed to amend the specification to provide antecedent basis for terminology used to describe elements/steps in the claims, which elements/steps were already supported by the originally-filed application. (See, e.g., Figs.1-3 and the supporting text spanning page 3, line 19 through page 8, line 28 of the originally-filed application.) As explained in the MPEP at Section 608.01(o), page 600-89 (Rev. 3, August 2005), "While an applicant is not limited to the nomenclature used in the application as filed, *he or she should make appropriate amendment of the specification*

whenever this nomenclature is departed from by amendment of the claims so as to have clear support or antecedent basis in the specification for the new terms appearing in the claims." (Emphasis added.)

It was therefore believed that these amendments would address all of the Office's concerns except for one, namely, the concern that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36." In response to this objection, Applicant's remarks noted that the Examiner had erred in parsing the claim. As amended, claim 36 does *not* define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device...." That is, the claimed system comprises two distinct elements (i.e., the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification were believed to be necessary to address this aspect of the Office's concern.

Despite having addressed the Examiner's stated concerns (i.e., lack of antecedent basis in the specification) upon which were based the objection to the specification and the rejection of claims under 35 U.S.C. §112, first paragraph, the Office issued an Advisory Action explaining that the proposed amendments to the specification would not be entered on the grounds that "they raise the issue of new matter." Accordingly, the issues of antecedent basis as well as new matter are addressed in the following discussion.

Because Applicant's proposed amendments to the specification were not entered, the specification does not include word for word support of the language presently recited in claims 1, 7, 19, 28, 36, and 44. However, it is well known that "the invention claimed does not have to be described in *ipsis verbis* in order to satisfy the description requirement of Sec. 112." In re Wright, 866 F.2d 422, 424 (Fed. Cir. 1989). Instead, it is sufficient if "the meaning of [the claim language in question] is sufficiently described in the specification to inform the public what said language is intended to encompass." *Id.*

It is respectfully asserted that the meaning of the claim language introduced in the amendment of January 5, 2006 was sufficiently described in the specification to satisfy all statutory requirements. In particular, the last paragraph of claim 1 was amended as follows:

using the cryptographic module of the mobile communications device[[,]] as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network.

Claim 7 was similarly amended to define "means for connection to a remote computer without involving the wireless communications network."

Claim 19 was amended to define:
the mobile communication device having a cryptographic module for use in mobile communication over a wireless communications network, such that the ~~mobile communications device~~ cryptographic module acts as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network

Claim 28 was amended to define "using the encrypted data in communications over the computer network without sending the encrypted data over the wireless communications network."

Claim 36 was amended to define:

wherein the cryptography service provider can obtain the cryptographic functionality, required by the application, from the cryptographic module of the mobile communications device without the mobile communications device sending the encrypted communications over the telecommunications network.

And claim 44 was amended to define:

wherein, in response to suitable commands received from the computer system over the second interface, the security manager module requests a cryptographic function from the cryptographic module, and returns the

results of the cryptographic function to the computer system over the second interface, without sending the results of the cryptographic function over the first wireless interface.

In each instance, the Office objected that the specification does not support claims that include a mobile communications device performing the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network.

This objection is without merit. For example, the specification at page 3, lines 26-30, expressly states that "[t]he computer has a connection to an external network 12, for example through a modem (not shown)." The connection to the network 12 is illustrated in FIG. 1, and it can clearly be seen that the connection does not involve the mobile station 30.

The text spanning page 3, line 31 through page 4, line 19 clearly sets forth an intention to provide cryptographic functionality to applications running in the computer, which applications are communicating with the network 12 via the computer's own connection to that network.

A solution, described in the specification text spanning page 4, line 20 through page 8, line 28 involves a mobile station 30 providing the desired cryptographic functionality for the computer. As described on page 6, lines 1-16, there is a communication link established between the computer and the mobile station so that the computer can request the desired functionality, and the mobile station can return the desired results.

It is clear from the description that the mobile station does not pass the cryptographic results on to its own wireless network, but rather returns these results to the computer. For example, FIG. 2 is a flowchart showing a method by which the PC 10 can use the cryptographic functionality in the mobile phone 30. As explained on page 8, lines 4-7 of the specification, "In step 112, the result of the operation in the MS 30 is sent to the CSP*26, and then to the CAPI 18. In step 114, the CAPI 114 [sic: 18], then responds to the application which requested the cryptographic functionality."

Since the application that requested the cryptographic functionality is using the computer's own connection to the network 12 (see e.g., FIG. 1), there is no need for the encrypted data to pass back through the mobile phone 32 to the wireless network. Thus, no such action is described in the specification.

That the mobile communications device performs the cryptographic function for the computer without sending the results of the cryptographic function over the wireless network

is further supported by the specification text at page 8, lines 8-28, in conjunction with FIG. 3, which is a flowchart showing the operation carried out in the MS 30. Of relevance here is that the MS 30 carries out the requested cryptographic operation (step 136), and "[t]hen, in step 138, the result of the cryptographic operation is sent back to the PC over the previously established communication link." It will be observed that sending the cryptographic operation result back to the PC is the final step carried out in the MS 30, because there is no need for the MS 30 to involve its own wireless network.

It should be clear from the foregoing remarks that the various instances of claim language defining a mobile communications device performing a cryptographic function for a computer without sending the results of the cryptographic function over the wireless network are well-supported in the specification.

As to the Office's additional allegation that "... the specification does not provide antecedent basis for the added limitation '*a computer including: ... a mobile communication device including a cryptographic module*', claimed within the amended claim 36," Applicant again respectfully asserts that the Examiner has erred in parsing the claim. As amended, claim 36 does not define the computer as including a mobile communication device. Rather, claim 36 defines "A system ...comprising: a computer ....; and a mobile communication device." That is, the claimed system comprises two distinct elements (i.e., the computer and the mobile communication device) which are separate from one another. The specification is replete with support for this arrangement. (See, e.g., Fig. 1.) Consequently, no further amendments to the specification are believed to be necessary to address the Office's concern.

Accordingly, it is respectfully requested that the objection to the specification as lacking antecedent basis, and the rejection of claims 1-19, 28-30, and 32-46 under the first paragraph of 35 U.S.C. §112 (regardless of whether the basis for the rejection is lack of antecedent basis or an allegation of new matter) be reversed.

Claims 19 and 47-50 stand rejected under 35 U.S.C. §101 as allegedly defining non-statutory subject matter. Specifically, regarding these claims, the Office considers the recitations of realizable or discernable modules to be merely recitations of software applications/instructions alone. This rejection is respectfully traversed.

During the above-referenced personal interview, the parties discussed the Section 101 rejection of claim 19. Applicant had earlier overcome a similar rejection of claim 19 by amending it to define "A tangible module ...." However, the Office now considers this language to be insufficient to satisfy the requirements of Section 101.

While Applicant does not agree with the Office's reasoning, new Amendments are now being presented in order to expedite favorable prosecution of the application. In particular, claim 19 has been amended to now define "A module for a personal computer, wherein the module is embodied in hardware ...." This amendment, which is supported in the specification at, for example, page 5, lines 29-30, eliminates software-only embodiments.

Independent claim 47 has also been amended to now define "A module ...comprising: ... an external interface, embodied in hardware, for connection to a mobile communication device containing a cryptographic module." (Emphasis added.) This amendment is supported in the specification at, for example, page 6, lines 8, which describes alternative hardware embodiments of the connection between the PC 10 and the mobile phone 30. The newly worded independent claim 47, as well as its dependent claims 48-50, is believed to overcome the Office's concern about software-only embodiments.

For at least the foregoing reasons, it is respectfully asserted that claims 19 and 47-50 satisfy the requirements of 35 U.S.C. §101. Therefore, it is respectfully requested that the rejection of these claims under Section 101 be withdrawn.

Claims 47 and 48 stand rejected under 35 U.S.C. §102(b) as allegedly being anticipated by Caputo et al. (U.S. Patent 5,778,071) (hereinafter "Caputo"). This rejection is respectfully traversed.

Claim 47 defines "A module for a computer system, the module comprising: an application interface ...; and an external interface, embodied in hardware, for connection to a mobile communication device containing a cryptographic module; *wherein, when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom.*" (Emphasis added.)

Claim 48 depends from 47 and further defines that "the module has some cryptographic functionality, and comprises means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function."

Neither of claims 47 and 48 is anticipated by Caputo because Caputo fails to disclose or suggest a division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device so that the computer comprises "a cryptographic module; wherein,

when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom," as defined by claim 47. Caputo is similarly silent with respect to claim 48's recitation of "*the module [having] some cryptographic functionality*, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function." (Emphasis added.)

The cited portions of Caputo merely describe two modes of operation: one in which the device 10 encrypts the data and immediately sends it to the network 20, and another in which the device 10 performs the encryption but then returns the encrypted data to the computer 22 for subsequent transmission to the network 20, possibly as part of another message. Nowhere does this passage describe a computer having its own cryptographic capabilities separate and apart from those provided by the device 10.

The Office Action appears to construe claims 47 and 48 as merely defining the computer sending commands to the cryptographic module. As to features such as "when the module receives from the application interface a request for a cryptographic function which the module is unable to provide, the module sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom," as defined by claim 47, and "the module [having] some cryptographic functionality, and compris[ing] means for determining in response to a request from the application interface whether it is able to provide the requested cryptographic function," as defined by claim 48, the Office Action states, on the top of page 26, that "the prior art shows separate elements in cooperation for the provision of cryptographic functionality. Thus the elements provide cryptographic functionality."

The Office's argument is, therefore, that Caputo anticipates the subject matter of claims 47 and 48 because Caputo's arrangement is capable of performing the same overall function as Applicant's arrangement. This is an improper basis for supporting the rejection because the test for anticipation is not whether two systems can perform the same function, but rather whether "each and every element *as set forth in the claim* is found, either expressly or inherently described, in a single prior art reference." *Verdegall Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053. (See MPEP §2131, page 2100-67 (Rev. 6, Sept. 2007.) The Office has failed to show how Caputo satisfies this requirement. For example, the Office has not shown where Caputo discloses a computer system having a

module that "has some cryptographic functionality", and also "sends a command over the external interface to the mobile communications device to request the cryptographic function therefrom" "when the module receives from the application interface a request for a cryptographic function which the module is unable to provide."

For at least the foregoing reasons, it is respectfully requested that the rejection of claims 47 and 48 under 35 U.S.C. §102(b) be withdrawn.

The Office made a number of rejections under 35 U.S.C. §103(a), which are addressed individually below. However, before presenting these arguments, it is noted that each of the rejections also appeared in a Final Office Action mailed on May 3, 2006, and Applicant responded to these in an Appeal Brief filed on November 24, 2006 (and re-filed on June 25, 2007 to overcome an informality). In response to a number of Applicant's arguments, the Office now states, "In response to applicant's arguments (A-C, E) against the references individually, one cannot show nonobviousness by attacking references individually where the rejections are based on combinations of references. [citation omitted]."

The Office's response is not understood. Applicant's arguments made previously (and repeated below) do not merely show that each reference, taken individually, is deficient in some way. Rather, in each case, Applicant shows that each reference lacks the same feature(s), so that any combination of the cited references would also lack the identified feature(s). This is a proper way to rebut an obviousness rejection, and it is requested that the Office keep this in mind when it reconsiders the following.

Claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Liebenow et al. (U.S. Patent 6,131,136) (hereinafter "Liebenow"). This rejection is respectfully traversed.

Embodiments defined by independent claims 1, 7, 19, 24, 28, 36 and 44 (as well as their related dependent claims 4, 6, 11, 13-15, 18, 26-27, 32-34, 37-39, and 42) are believed to be patentably distinguishable over the prior art of record because they include novel and nonobvious features that enable a single mobile communications device to achieve a unique efficiency in that *a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1.* In this respect, it is important to understand that the personal computer is *not* communicating *through* the mobile

communications device and the wireless network to get to its own network; its exchanges with the mobile communications device are merely for the purpose of utilizing the cryptographic functions that the mobile communications device can offer.

Specific claimed features lacking in Caputo and Liebenow are discussed in the following sections A through E, followed by an additional discussion of why the Liebenow patent does not make up for the deficiencies of Caputo.

A. Neither Caputo nor Liebenow et al. disclose "establishing a connection with a mobile communications device, wherein said mobile communications device includes a cryptographic module for use in mobile communication"

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because *a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network,* but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. To that end, independent claim 1 defines "establishing a connection with a mobile communications device, wherein said mobile communications device includes a *cryptographic module for use in mobile communication*," (emphasis added) and each of independent claims 7, 19, 24, 28, 36, and 44 uses the same or similar language to define a comparable feature. Neither of the Caputo or Liebenow documents discloses or suggests this feature.

In support of its rejection, the Office Action asserts that Caputo discloses this claimed feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38.

Applicant respectfully disagrees because the cryptographic circuitry disclosed by Caputo is not "for use in mobile communication over a wireless communications network" as variously required by the claims. Instead, the Caputo device requires a wired connection to a network. (See, e.g., Fig. 2 and column 5, lines 62-65: "Further, the connector port 14 is a modular receptacle which may be directly connected to a data transfer path, such as a telephone system.") Thus, there would be absolutely no need for Caputo's cryptographic circuitry to be for use in mobile communication over a wireless communications network.

Liebenow fails to make up for the deficiencies of Caputo at least because it does not even discuss cryptography. Consequently, any combination of Caputo with Liebenow would still lack this feature.

B. Neither Caputo nor Liebenow disclose "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"

As mentioned earlier, an aspect of the variously claimed embodiments is that a single mobile communications device is able to achieve a unique efficiency because a same cryptographic module located in the mobile communications device is used not only to support the device's own communications with a wireless network, but also the cryptography requirements of a local external device, such as a personal computer having its own connection with a network as illustrated in FIG. 1. When the mobile communications device is operating on its own behalf, its encrypted communications can be sent over the wireless communications link. However, when the mobile communications device is operating for the benefit of the computer, it merely returns the encrypted result to the computer without involving the wireless communications network. Independent claims 1, 7, 19, 28, 36, and 44 thus variously define "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network."

The Office Action asserts that Caputo discloses this feature at figure 3; column 9, lines 46-60; column 15, lines 13-39; column 2, lines 23-27; and column 3, lines 33-38. Applicant respectfully disagrees because one principle of operation taught by Caputo is that Caputo's computer is connected to the network *through* the device 10 (see, e.g., Caputo et al.'s figure 2). Consequently, even if the Caputo device 10 were modified to have wireless mobile communications capability (i.e., communicating with a wireless network), the external device 10 of Caputo would still be the computer's only path to the network. Thus, the computer would have to use the hypothetically-modified wireless mobile communications device to access its computer network through the wireless communications network. Such use would be contrary to the requirement that the cryptographic module be used to "encrypt[]

said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network." Liebenow fails to make up for the deficiencies of Caputo at least because it, too, is a pass-through device, and does not suggest returning any cryptographic results to the attached computer.

C. Neither Caputo nor Liebenow disclose a dual-mode cryptographic module that is both "for use in mobile communication over a wireless communications network" and also "us[ed] ... as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network"

Independent claim 1 defines "a cryptographic module for use in mobile communication over a wireless communications network" and also "using the cryptographic module of the mobile communications device as a cryptographic service provider for encrypting said communications from said computer over said computer network without sending said encrypted communications over said wireless communications network." Independent claims 7, 19, 24, 28, 36, and 44 variously define comparable features. Neither Caputo nor Liebenow discloses or suggests this feature, and any combination of these two teachings would similarly lack the claimed limitations.

The device of Caputo appears to operate in only one mode, namely, for the benefit of the external device (computer); it sits in-between the computer and the network, passing data from one to the other, and performs cryptographic functions as required by the node that the *computer* is connected to. Consequently, there is no dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network." Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography, and therefore cannot suggest a dual-mode cryptographic module as claimed.

D. Neither Caputo nor Liebenow disclose a system in which "a first part of the required cryptographic functionality [is] provided in the computer, and a second part of the required cryptographic functionality [is] provided in the mobile communications device"

Independent claim 24 further defines "a first part of the required cryptographic functionality being provided in the computer, and a second part of the required cryptographic functionality being provided in the mobile communications device."

As explained earlier with respect to the rejection of claims 47 and 48, Caputo fails to disclose or suggest this claimed feature because it is silent with respect to any division of cryptographic functions wherein some are performed within the computer itself and others are performed within a cryptographic module located in a mobile communications device.

Liebenow fails to make up for the deficiencies of Caputo because it is silent with respect to cryptography. Consequently, any combination of Caputo with Liebenow would still lack the claimed feature.

E. Neither Caputo nor Liebenow disclose a system in which "the computer further compris[es] an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto"

Claim 24 additionally defines "the computer further comprising an interface device which, on determining that an application needs to use cryptographic functionality, selects the functionality provided in the computer, or the functionality provided in the mobile communications device, and sends a command thereto." This feature is related to the feature discussed above in Section D, wherein a first part of the required cryptographic functionality is provided in the computer, and a second part of the required cryptographic functionality is provided in the mobile communications device. The claimed "interface" provides the capability of selecting which of the two cryptographic functionality service providers will be used when needed.

As Caputo is lacking any disclosure of some cryptographic functionality being performed in the computer, and some cryptographic functionality being performed in the mobile communications device, it follows that Caputo does not describe an interface for

selecting one of the two. Liebenow, which is silent with respect to cryptographic functionality, fails to make up for the deficiencies of Caputo.

F. Any combination of Caputo's teachings with the teachings of Liebenow would still lack features variously defined by Applicant's claims

The Office Action acknowledges that Caputo does not disclose, at least, a mobile communication device that is also usable over a wireless communications network, but relies on Liebenow as making up for this deficiency. This reliance is unfounded, at least for the reasons discussed above in Sections A through E.

Moreover, Applicant believes that Liebenow cannot be considered to disclose a mobile communication device, as that term is used in Applicant's specification. Instead, Liebenow discloses a dual mode modem that automatically switches between a wireless and wire-based communication modes using mode selection circuitry that detects when a wire-based communications network, such as a standard land-line telephone network, is coupled to the modem. Such a device fails to satisfy Applicant's variously-worded definitions of "said mobile communications device includ[ing] a cryptographic module for use in mobile communication over a wireless communications network." (See, e.g., independent claims 1, 7, 19, 24, 28, 36, and 44.) Rather, Liebenow's dual mode modem is more of a dumb, slave device that could never be used on its own; it would therefore never require its own cryptographic module *for use in mobile communication over a wireless communications network*, as required by Applicant's claims. Consequently, any combination of Caputo with Liebenow would still lack this claimed feature.

Moreover, even if Caputo's device were modified to include Liebenow's dual mode capability, the combination would still operate in only one mode, namely, for the benefit of the external device (computer), operating only to pass data between the computer and its network. All cryptographic functions would be performed only as required by the node that the *computer* is connected to, *and would pass through the device to the computer network.* By contrast, embodiments such as those defined by independent claim 28 require that *the encrypting device return the encrypted data to the computer* for communication over a computer network without sending the encrypted data over the wireless communication network. See also independent claim 44, which defines "a mobile communications device ... comprising a security manager module ... *[that] returns the results of the cryptographic function to the computer system* ...." (Emphasis added.) Consequently, any combination of

Caputo with Liebenow et al. would still lack any dual mechanism in which the cryptographic module of the mobile communication device is "for use in mobile communication over a wireless communications network" and also for "[acting] as a cryptographic service provider for said personal computer allowing the personal computer to communicate encrypted data over said computer network without sending data over said wireless communications network."

G. Conclusion

For at least the foregoing reasons, claims 1, 4, 6, 7, 11, 13-15, 18, 19, 24, 26-28, 32-34, 36-39, 42, and 44 are believed to define subject matter that is patentably distinguishable over any combination of Caputo and Liebenow. Therefore, it is respectfully requested that the rejection of these claims under 35 U.S.C. §103(a) be withdrawn.

Claims 5, 8, 9, 41, and 46 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Ericsson, "Bluetooth -- A Global Specification for Wireless Connectivity" (hereinafter "Ericsson"). This rejection is respectfully traversed.

Claims 5, 8-9, 41, and 46 variously depend from independent claims 1, 7, 36, and 44 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its disclosing the use of Bluetooth technology, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Ericsson would still lack the various combinations of elements defined by claims 5, 8, 9, 41, and 46.

For at least the foregoing reasons, Claims 5, 8-9, 41, and 46 are believed to define subject matter that is novel and nonobvious over any combination of Caputo with Liebenow and Ericsson. It is therefore respectfully requested that the rejection of claims 5, 8, 9, 41, and 46 under 35 U.S.C. §103(a) be withdrawn.

Claim 49 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of Ericsson. This rejection is respectfully traversed.

Claim 49 depends from independent claim 47 and is therefore patentably distinguishable over any combination of Caputo for at least the reasons discussed above. Furthermore, the Ericsson document, which was relied on by the Office merely for its

disclosing the use of Bluetooth technology, also fails to disclose any of the above-identified features that are lacking in Caputo. Consequently, any combination of Caputo with Ericsson would still lack the combinations of elements defined by claim 49.

For at least the foregoing reasons, Claim 49 is believed to define subject matter that is novel and nonobvious over any combination of Caputo with Ericsson. It is therefore respectfully requested that the rejection of claim 49 under 35 U.S.C. §103(a) be withdrawn.

Claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of Geiger et al. (US Patent 6,463,534 B1) (hereinafter, "Geiger"). This rejection is respectfully traversed.

Claims 2-3, 10, 12, 16, 17, 25, 29-30, 35, and 40 variously depend from independent claims 1, 7, 24, 28, and 36 and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the Geiger document, which was relied on by the Office merely for its disclosing the use of the Wireless Application Protocol (WAP) (utilizing WTLS and a WIM), also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with Liebenow and Geiger would still lack the various combinations of elements defined by claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40.

For at least the foregoing reasons, claims 2, 3, 10, 12, 16, 17, 25, 29, 30, 35, and 40 are believed to define subject matter that is patentably distinguishable over any combination of Caputo with Liebenow and Geiger. It is therefore respectfully requested that the rejection of these claims under 35 U.S.C. §103(a) be withdrawn.

Claims 43 and 45 stand rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over the combination of Caputo and Liebenow in view of RSA, "PKCS #11 v2.10: Cryptographic Token Interface Standard" (hereinafter "RSA"). This rejection is respectfully traversed.

Claims 43 and 45 depend from independent claims 36 and 44, respectively, and are therefore patentably distinguishable over any combination of Caputo and Liebenow for at least the reasons discussed above with respect to these base claims. Furthermore, the RSA document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to

the base claims. Consequently, any combination of Caputo with Liebenow and RSA would still lack the various combinations of elements defined by claims 43 and 45.

For at least the foregoing reasons, claims 43 and 45 are believed to define subject matter that is patentably distinguishable over any combination of Caputo with Liebenow and RSA. It is therefore respectfully requested that the rejection of these claims under 35 U.S.C. §103(a) be withdrawn.

Claim 50 stands rejected under 35 U.S.C. §103(a) as allegedly being unpatentable over Caputo in view of RSA. This rejection is respectfully traversed.

Claim 50 depends from independent claim 47, and is therefore patentably distinguishable over Caputo for at least the reasons discussed above with respect to claim 47. Furthermore, the RSA document, which was relied on by the Office merely for its disclosing the use of PKCS #11 with AT commands, also fails to disclose any of the features discussed above with respect to the base claims. Consequently, any combination of Caputo with RSA would still lack the combination of elements defined by claim 50.

For at least the foregoing reasons, claim 50 is believed to define subject matter that is patentably distinguishable over any combination of Caputo with RSA. It is therefore respectfully requested that the rejection of this claim under 35 U.S.C. §103(a) be withdrawn.

New claims 51 and 52 have been added to the application without introduction of new matter. At the suggestion of the Examiner (made in the personal interview referenced above), these claims incorporate the use of a SIM-WIM card to distinguish over the prior art of record. In particular, these claims define "using the cryptographic module on the SIM-WIM card to carry out the encryption operation" when a node accessed by the mobile communications device via a wireless network requires performance of an encryption operation, and also when a local external device having a connection to a network by means other than the mobile communication device requires performance of an encryption operation. Support for the use of a SIM-WIM card in this manner can be found in the specification at, for example, page 4, line 35 through page 5, line 5 (performing cryptographic functionality for the phone's own connections); page 5, lines 12-15 (embodying the phone's cryptographic capability on a SIM-WIM card); and page 5, lines 22-28 (the phone is used as a cryptography service provider). The subject matter defined by claims 51 and 52 is believed to be patentably distinguishable over the prior art of record.

The application is believed to be in condition for allowance. Prompt notice of same is respectfully requested.

Respectfully submitted,

Potomac Patent Group PLLC

Date: January 3, 2008

By: /Kenneth B. Leffler, Reg. No. 36,075/
Kenneth B. Leffler
Registration No. 36,075

P.O. Box 270
Fredericksburg, Virginia 22404
703-718-8884